

معاونت پژوهش، برنامه‌ریزی و سنجش مهارت

دفتر پژوهش، طرح و برنامه‌ریزی درسی

استاندارد آموزش شغل

مهندس کامپیوتر در امنیت کسب و کار الکترونیکی

گروه شغلی

فناوری اطلاعات

کد ملی آموزش شغل

۲	۵	۲	۹	۴	۰	۵	۳	۱	۷	۵	۰	۰	۰	۱
ISCO-۰۸				سطح مهارت	شناسه گروه			شناسه شغل			شناسه شایستگی			نسخه

۰-۲۳/۹۷/۱/۲

تاریخ تدوین استاندارد : ۸۴/۶/۱

**تعریف مفاهیم سطوح یادگیری**

آشنایی: به مفهوم داشتن اطلاعات مقدماتی/شناسایی: به مفهوم داشتن اطلاعات کامل/اصول: به مفهوم مبانی مطالب نظری/ توانایی: به مفهوم قدرت انجام کار

مشخصات عمومی شغل:

مهندس کامپیوتر در امنیت کسب و کار الکترونیکی کسی است که روشهای بنیادین مورد استفاده در کاهش مخاطرات امنیتی E-Business را بوجود آورد و ایمن سازی کاربران تحت وب، سرویس دهنده ها و ارتباطات و کنترل استفاده از فایروالها و تاییدیه های دیجیتال را انجام می دهد. همچنین از عهده بررسی و شناخت Information Security در مهندسی نرم افزار، کار با نیازمندی های Security، کار با Risk Management و Ethical و Professional Issues در Information Security، کار با Risk Management، کار با Security Management، کار با Assessing و Controlling Risk در Risk Management، کار با Blueprint برای Security، کار با Continuity Planning برای Continuity، کار با فناوری های Security، کار با Physical Security، پیاده سازی Security، انجام Information Security Maintenance، کار با Security و Personnel بر خواهد آمد. مهندس کامپیوتر E-Security مراکز کامپیوتر و IT در تیم های مهندسی نرم افزار برای طراحی و پیاده سازی سیستم های مهندسی نرم افزار برای امنیت M-Commerce و E-Commerce و E-Business و E-Commerce و E-Learning و Government و موارد دیگر در مراکز میتواند انجام وظیفه کند.

ویژگی های کارآموزورودی:

حداقل میزان تحصیلات: مهندس کامپیوتر

حداقل توانایی جسمی: متناسب با نوع شغل

مهارت های پیش نیاز این استاندارد: -

طول دوره آموزشی:

طول دوره آموزش	:	۲۶۴	ساعت
- زمان آموزش نظری	:	۲۳	ساعت
- زمان آموزش عملی	:	۸۱	ساعت
- زمان کارآموزی در محیط کار	:	۸۰	ساعت
- زمان اجرای پروژه	:	۸۰	ساعت
- زمان سنجش مهارت	:	-	ساعت

روش ارزیابی مهارت کارآموز:

۱- امتیاز سنجش نظری (دانش فنی): ۲۵٪

۲- امتیاز سنجش عملی: ۷۵٪

۱-۲- امتیاز سنجش مشاهده ای: ۱۰٪

۲-۲- امتیاز سنجش نتایج کار عملی: ۶۵٪

ویژگیهای نیروی آموزشی:

حداقل سطح تحصیلات: لیسانس مرتبط



سازمان آموزش فنی و حرفه‌ای کشور

نام شغل: مهندس کامپیوتر در امنیت کسب و کار الکترونیکی

فهرست توانایی های شغل

ردیف	عنوان توانایی
۱	توانایی بررسی و شناخت Information Security در مهندسی نرم افزار
۲	توانایی کار با نیازمندی های Security
۳	توانایی کار با Legal و Ethical و Professional Issues در Information Security
۴	توانایی مدیریت مخاطرات
۵	توانایی کار با Assessing و Controlling Risk در Risk Management
۶	توانایی کار با Blueprint برای Security
۷	توانایی Continuity Planning برای Security
۸	توانایی کار با تکنولوژی های Security
۹	توانایی کار با Physical Security
۱۰	توانایی پیاده سازی Security
۱۱	توانایی انجام Information Security Maintenance
۱۲	توانایی کار با Security و Personnel

زمان آموزش			شرح	شماره
جمع	عملی	نظری		
۴/۵	۳	۱/۵	<p>توانایی بررسی و شناخت Information Security درمهندسی نرم افزار</p> <p>۱-۱ آشنایی با مفاهیم اولیه و اساسی information security</p> <p>۱-۲ آشنایی با بررسی computer security و زیر سیستم آن information security</p> <p>۱-۳ آشنایی با موارد کلیدی و مشکلات information security</p> <p>۱-۴ شناسایی اصول بررسی security systems و نقش آن در development life cycle در مهندسی نرم افزار</p> <p>۱-۵ شناسایی اصول بررسی موارد پیشرفته و حرفه ای information security در ساختار سازمان</p>	۱
۴/۵	۳	۱/۵	<p>توانایی کار با نیازمندی های Security</p> <p>۲-۱ شناسایی اصول تنظیم نیازمندیهای business برای information security</p> <p>۲-۲ شناسایی اصول برنامه ریزی و طرح موفق information security برای پاسخ به مدیر عمومی و مدیر کامپیوتر و IT</p> <p>۲-۳ شناسایی اصول بررسی threats posed برای information security</p> <p>۲-۴ شناسایی اصول بررسی تفاوت بین تهدید information systems و حمله به information systems</p>	۲
۹	۵	۴	<p>توانایی کار با Legal و Ethical و Professional Issues در Information Security</p> <p>۳-۱ شناسایی اصول بررسی تفاوت بین ethics و laws</p> <p>۳-۲ شناسایی اصول بررسی و کار با national laws که برای information security</p> <p>۳-۳ شناسایی اصول کار با role های یک فرهنگ برای information security</p>	۳
۸	۶/۵	۱/۵	<p>توانایی مدیریت مخاطرات</p> <p>۴-۱ شناسایی اصول کار با risk management و role ها در SecSDLC</p> <p>۴-۲ شناسایی اصول کار با risk و شناسایی آن</p>	۴



زمان آموزش			شرح	شماره
جمع	عملی	نظری		
			شناسایی اصول ارزیابی risk در احتمال رویداد و گیر انداختن در یک سازمان	۴-۳
			شناسایی اصول اعمال دیدگاه سخت در شناسایی documenting risk و assessment	۴-۴
۴/۵	۳	۱/۵	<p>توانایی کار با Assessing و Controlling Risk در Risk Management</p> <p>شناسایی اصول تشخیص چگونگی risk control برای نیاز سازمان</p> <p>شناسایی اصول کار با گزینه های استراتژی risk mitigation برای controlling risks</p> <p>شناسایی اصول کارشناخت جزئیاتی که برای classify Controls بکار میروند</p> <p>که conceptual frameworks شناسایی اصول کار با آگاهی برای موجود است و توانا هستند برای فرمول risk controls برای ارزیابی کردن قیمت آنالیز سودمند</p> <p>شناسایی اصول انجام maintain و perpetuate برای risk controls</p>	<p>۵</p> <p>۵-۱</p> <p>۵-۲</p> <p>۵-۳</p> <p>۵-۴</p> <p>۵-۵</p>
۸	۶/۵	۱/۵	<p>توانایی کار با Blueprint برای Security</p> <p>شناسایی اصول کار با management's responsibilities و role در development و maintenance و enforcement در خصوص سیاست information security و standards و guidelines</p> <p>شناسایی اصول کار با سیاستهای کلی سازمان بین information security requirements و اهداف و سیاست های ویژه سازمان</p> <p>شناسایی اصول کار با blueprint یک information security در خصوص major components</p> <p>شناسایی اصول کار با policies و standards و عادات استفاده از آموزش و کآموزی و برنامه های آگاهی</p> <p>شناسایی اصول کار با information security architecture مناسب</p>	<p>۶</p> <p>۶-۱</p> <p>۶-۲</p> <p>۶-۳</p> <p>۶-۴</p> <p>۶-۵</p>

زمان آموزش			شرح	شماره
جمع	عملی	نظری		
۸	۶/۵	۱/۵	<p>توانایی برای Continuity Planning</p> <p>۷-۱ شناسایی اصول کار با contingency planning و incident response planning و disaster recovery planning و business continuity plans</p> <p>۷-۲ شناسایی اصول کار با المنت های business impact analysis و information که برای attack profile گردآوری میشوند</p> <p>۷-۳ شناسایی اصول کار با اجزاء incident response plan</p>	۷
۴/۵	۳	۱/۵	<p>توانایی کار با تکنولوژی های Security</p> <p>۸-۱ شناسایی اصول کار با انواع firewalls</p> <p>۸-۲ شناسایی اصول دستیابی به firewall implementation</p> <p>۸-۳ شناسایی اصول دستیابی به dial-up access و protection</p> <p>۸-۴ شناسایی اصول کار با دو عامل intrusion detection systems</p> <p>یعنی Identify و describe</p> <p>۸-۵ شناسایی اصول کار با دو استراتژی behind intrusion detection systems</p>	۸
۴/۵	۳	۱/۵	<p>توانایی کار با Physical Security</p> <p>۹-۱ شناسایی اصول کار با نیازمندی های physical security</p> <p>۹-۲ شناسایی اصول شناسایی تهدید برای information security و unique کردن physical security</p> <p>۹-۳ شناسایی اصول کار با موارد کلیدی physical security برای انتخاب یک facility site</p> <p>۹-۴ شناسایی اصول کار با اجزای physical security monitoring</p> <p>۹-۵ شناسایی اصول کار با المنت های لازم access control در داخل facilities management حوزه</p> <p>۹-۶ شناسایی اصول کار با criticality در خصوص برنامه های fire safety برای همه برنامه های physical security</p>	۹

زمان آموزش			شرح	شماره
جمع	عملی	نظری		
۲۴	۲۰	۴	<p>توانایی پیاده سازی Security</p> <p>۱۰-۱ شناسایی اصول برنامه ریزی و طرح security سازمان با یک project plan</p> <p>۱۰-۲ شناسایی اصول بررسی سازمان از نظر security با استفاده از آدرس دهی project plan</p> <p>۱۰-۳ شناسایی اصول تهیه significant role و اهمیت project information security project manager در موفقیت</p> <p>۱۰-۴ شناسایی اصول گردآوری نیازمندی های professional project complex projects برای management</p> <p>۱۰-۵ شناسایی اصول گردآوری استراتژی های تکنیکی و مدلها برای پیاده سازی project plan</p> <p>۱۰-۶ شناسایی اصول گردآوری مسائل غیر تکنیکی که چهره سازمان را در هر زمان تغییر میدهند</p>	۱۰
۱۶/۵	۱۵	۱/۵	<p>توانایی انجام Information Security Maintenance</p> <p>۱۱-۱ شناسایی اصول شناخت نیازمندی ها برای ادامه حفظ maintenance information security برای برنامه</p> <p>۱۱-۲ شناسایی اصول کار با مدلهاى security management توصیه شده</p> <p>۱۱-۳ شناسایی اصول کار با مدلهاى گوناگون برای برنامه کامل maintenance</p> <p>۱۱-۴ شناسایی اصول کار با فاکتورهای کلیدی برای monitoring برای محیط های internal و external</p> <p>۱۱-۵ شناسایی اصول انجام planning و risk assessment در یک information security maintenance</p> <p>۱۱-۶ شناسایی اصول کار vulnerability assessment و آموزش information security maintenance</p> <p>۱۱-۷ شناسایی اصول کار آموزش build readiness و and review information security procedures در داخل maintenance</p>	۱۱

زمان آموزش			شرح	شماره
جمع	عملی	نظری		
۸	۶/۵	۱/۵	<p>توانایی کار با Personnel و Security</p> <p>۱۲-۱ شناسایی اصول بررسی مکان و زمان اجرای عملیات information security در یک سازمان</p> <p>۱۲-۲ شناسایی اصول یافتن کارمندانی که وابستگی و ملاک عملیاتی information security هستند</p> <p>۱۲-۳ شناسایی اصول کار بر روی استوار نامه حرفه ای که در information security field میتواند برقرار گردد</p> <p>۱۲-۴ شناسایی اصول کار با مواردی که میتواند سیاست گذاری برای کارمندان را قانونی کند و تمرین برای پشتیبانی information security</p> <p>۱۲-۵ شناسایی اصول کار اقدامات حیاطی لازم برای افراد غیر کارمند</p> <p>۱۲-۶ شناسایی اصول تنظیم مستندات قانونمند کردن نیازها برای دسته بندی وظایف</p> <p>۱۲-۷ شناسایی اصول تنظیم مستندات نیازمندی های ویژه برای personnel data بسیا تر محرمانه</p>	



فهرست استاندارد تجهیزات، ابزار، مواد و وسایل رسانه ای

ردیف	مشخصات فنی	تعداد	شماره
۱	کامپیوتر پنتیوم IV کامل یا مشابه یا بالاتر برای Windows Xp	۸	
۲	کامپیوتر پنتیوم IV کامل یا مشابه یا بالاتر برای Windows 2003 server	۸	
۳	کامپیوتر پنتیوم IV کامل یا مشابه یا بالاتر برای Linux	۸	
۴	CD های MS Office Xp	۸	
۵	Cisco PIX FireWall	۸	
۶	چاپگر	۸	
۷	CD های آموزشی	۸	
۸	پوستر	۸	



ردیف	شرح
۱	کلیه سایتهای اینترنتی بهترین مرجع و منبع برای امنیت کسب و کار الکترونیک میباشند.
۲	http://www.cisco.com
۳	http://www.symantec.com
۴	http://www.mcafee.com
۵	http://www.redhat.com
۶	http://www.microsoft.com
۷	http://www.astalavista.com
۸	http://www.antivirus.com
۹	http://www.oracle.com
۱۰	انواع کتابها و نرم افزارهای آموزشی مربوط به Hack و Crack و Security و Virus و Firewall و مدیریت نیروها و امکانات در وضعیتهای بحرانی
۱۱	بانکها و موسسات مالی
۱۲	شرکتهای کارگذاری الکترونیکی
۱۳	فروشگاههای الکترونیکی
۱۴	حراجیههای الکترونیکی
۱۵	بورس نفت
۱۶	بورس ارز
۱۷	بورس کالاهای صنعتی
۱۸	بورس کالاهای کشاورزی
۱۹	بورس اوراق بهادار
۲۰	شرکتهای سرمایه گذاری
۲۱	شرکتهای سرویس دهنده اینترنت (ISP) و (ICP)